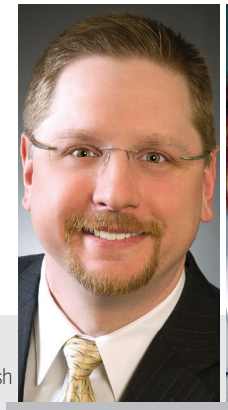
Be prepared

How implementing cybersecurity plans can protect against threats

INTERVIEWED BY JAYNE GEST



CARL A. KESSLER III
Senior vice president, CIO
First Federal Lakewood
(216) 529-2990
ckessler@ffl.net

BONNY CARROLL
Assistant vice president, Cash Management Public Funds
First Federal Lakewood
(216) 529-2622
bcarroll@ffl.net

WEBSITE: For more information about the First Federal Lakewood Commercial Banking Team, visit www.FFL.net.

Insights Banking & Finance is brought to you by **First Federal Lakewood**

As cybersecurity threats intensify, protecting your company's financial accounts is a priority. We often hear about large company data breaches but attacks that use the same tactics are also on the rise for small and midsize businesses.

"Smaller businesses can be easy for cybercriminals to exploit because they often lack basic controls or have poorly configured controls," says Carl A. Kessler III, senior vice president and CIO at First Federal Lakewood. "It is essential to work with your bank to protect your organization."

"It's our job to understand a customer's normal money flow — where it comes in from, where it should be going out and in what channels these typically happen," says Bonny Carroll, assistant vice president, Cash Management Public Funds. "Then we set up the appropriate products with thresholds, dual controls and processes to enable client protection. Your bank needs to invest time to understand your business, which helps you mitigate risks over time."

Smart Business spoke with Kessler and Carroll about minimizing the potential for cyberattacks on your financial accounts.

What types of attacks are becoming more prevalent for smaller organizations and why?

Two types of threats are increasing in particular — point-of-sale (POS) system compromise, which involves credit card information that is stolen, often from major retailers, and coordinated, sophisticated attacks that aim to wire transfer funds from your company to international accounts.

With POS system fraud, cybercriminals use automation to distribute malware very efficiently. A small restaurant chain with four POS systems and poor controls is an easier target than a larger retailer. With little cost for distribution, attacking many smaller targets becomes attractive. As the new EMV or 'chip' cards become more prevalent, it will get harder to commit POS fraud — so there's a push to exploit the gap now.

Wire transfer has a higher pay-off and criminals are getting more sophisticated. Surveillance can take months, as they learn when your account balances are highest, such as prior to payday. The cybercriminals also may deploy multiple techniques to facilitate the fraud. For instance, they use malware to steal one user ID and password, as well as a second person's credentials if you have dual controls. At the moment of attack they coordinate with a distributed denial of service attack on the bank. This is a smokescreen that provides time to move the funds. By the time the smoke settles, the money is gone.

How can businesses guard against threats?

Systems with default user IDs and passwords are a common way that criminals gain initial entrance, but there are ways to protect information and combat data breach threats. A cybersecurity firm can provide a comprehensive security assessment to identify vulnerabilities. You can then devise a plan to firm up systems and controls, which may include implementing dual controls; regularly changing passwords and ensuring they aren't easy to guess; and keeping machines patched and anti-virus software up-to-date.

It's also essential to have effective security for mobile devices, especially for executives. Phones have been stolen and used to mimic an executive, asking employees to bypass controls and send money immediately. Follow procedures in all cases — nobody, not even the CEO, should be allowed to override your best practices.

Stay current on your online banking balances, and know your business cycles — when you have the highest account balances, be extra vigilant and contact your bank right away if anything seems out of the ordinary. If you take credit cards, evaluate how quickly you can move to the EMV machines.

What help should your bank provide?

You need to establish good communication with your bank and discipline in monitoring account activity. By sharing information with the bank about typical account cycles, both of you know what to expect and can, therefore, identify suspicious activity sooner. Fraud prevention products, like Positive Pay, automate daily communication by providing the bank a list of checks and automated clearinghouse items issued; the bank reconciles the list as items are presented.

You also can set up a daily wire limit that restricts the amount permitted to transfer, keeping in mind that a limit has to be meaningful to protect yourself as intended. ●